

Vulnerability Information Coordination and Disclosure Policy

KUBOTA Corporation

I. Overview

The Kubota Corporation Product Security Incident Response Team (hereinafter referred to as Kubota-PSIRT) is responsible for receiving, evaluating, and responding to vulnerability information related to products and services manufactured and provided by the company.

This policy outlines our approach to handling reported vulnerability information, with the aim of enhancing the security of our products and providing users with appropriate risk mitigation measures.

While we design our products with security in mind during development, this policy is intended to facilitate the acceptance of reports from users in the event that vulnerabilities are discovered.

This policy may be revised without prior notice.

II. Scope

This vulnerability disclosure policy applies only to vulnerabilities in the following products and services.

The applicable period is from the product's release until the end of its support period (10 years).

The scope of this policy is limited to Kubota brand agricultural and construction machinery products, their associated software and services, and the supporting infrastructure, including databases and servers.

III. Reporting Vulnerability Information

1. Dedicated Contact Point for Vulnerability information reporting contact

Please report any vulnerability information to Kubota-PSIRT using the following method:

- [Vulnerability Submission Form](#)

2. Acknowledgment and response

- As a general rule, we will acknowledge receipt of reports within 5 business days of receiving them.
- Please note that if no contact information is provided in the customer information field, we will be unable to acknowledge receipt and share progress updates.
- The company will not take legal action against reports made in good faith.

- Additional information may be requested, if necessary.
- The company does not operate a bug bounty program (reward system).

IV. Definition of Vulnerability

In this policy, a “vulnerability” refers to any issue that may adversely affect confidentiality, integrity, or availability due to program bugs, design flaws, or similar defects in our products (such as software, hardware, and firmware).

V. Information Required for Reporting

To facilitate smooth reporting, please provide the following information to the extent possible.

1. Applicable product and version information (the product’s URL, lot number, etc.)
2. Circumstances of vulnerability discovery (tools used, verification environment, etc.)
3. Reproduction steps and PoC (Proof of Concept)
4. Expected impact and threat scenarios
5. Whether public disclosure is planned and the timing of such disclosure (e.g., conference presentation, blog post, etc.)

VI. Post-report Response Policy

- Kubota-PSIRT will review the reported details and collaborate with relevant departments to assess the impact and consider countermeasures.
- Support type: Update or replace ECU software.
- Support method: Distribute security patches via sales companies/dealers to implement ECU security measures.
- If the issue arises from a third-party component, we will coordinate with the relevant vendor and coordination organizations (e.g., JPCERT/CC).
- We will regularly share progress updates with the reporter. (every 30 days or more frequently)
- The regular progress updates mentioned above will be communicated via email, telephone, or other appropriate means.

VII. Vulnerability Information Disclosure Policy

- After completing the response, Kubota-PSIRT will disclose the following information on the company's official website.

[List of vulnerabilities and incidents](#)

- Applicable product and version
- Overview of the vulnerability (excluding technical details, such as exploit code and information that could lead to unauthorized use)
- Scope of impact and countermeasures
- CVE number (if applicable)
- The CVE number will be obtained in coordination with [JPCERT/CC](#) and communicated to the reporter.
- Credit will be given to the reporter, if requested.
(anonymous reporting is also acceptable).

VIII. Revision history

- 06 05, 2026: Initial version established